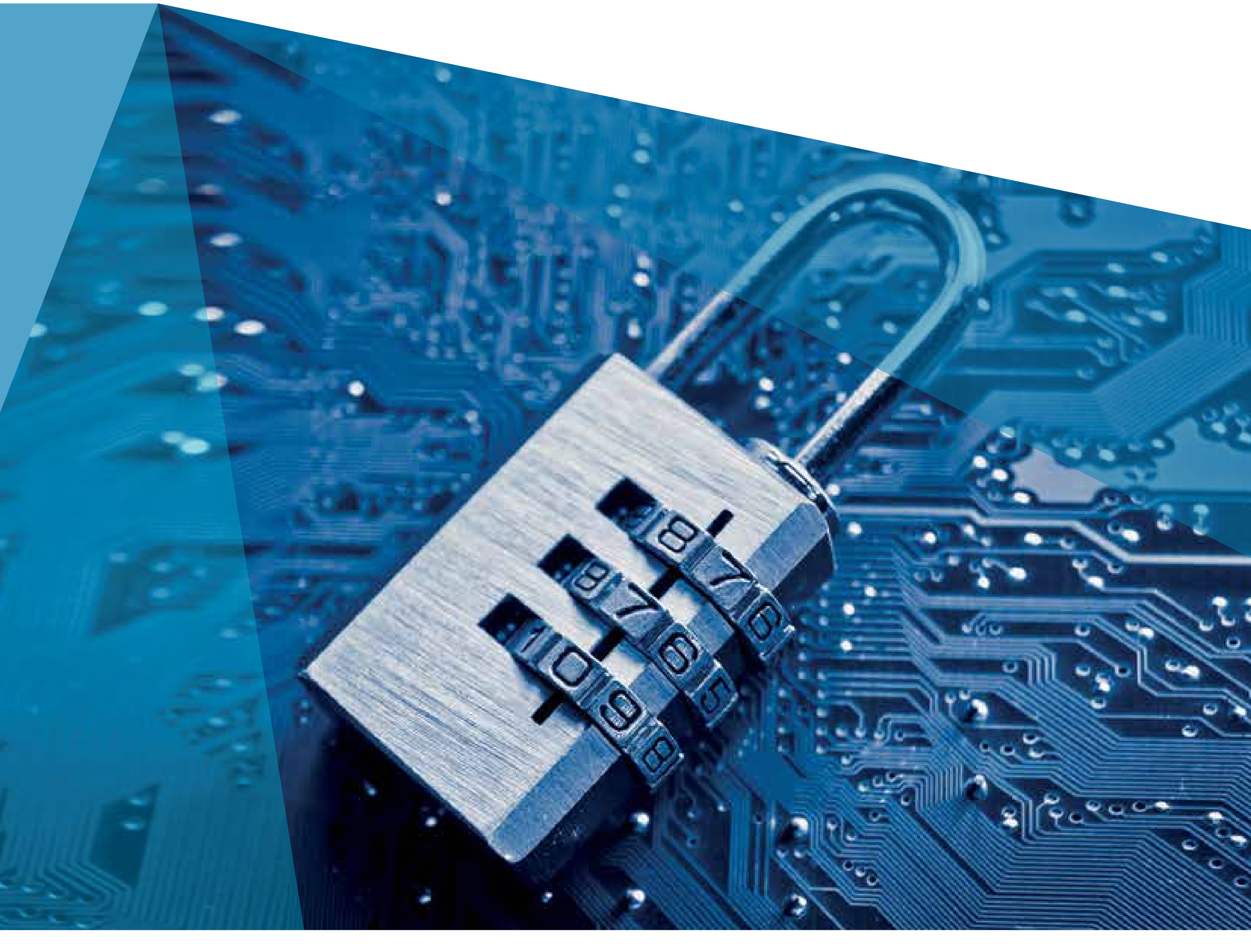
OLIVER WYMAN

CLOSING THE DOOR TO CYBER ATTACKS

HOW ENTERPRISES CAN IMPLEMENT COMPREHENSIVE INFORMATION SECURITY



MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

CLOSING THE DOOR TO CYBER ATTACKS

Cybersecurity and information security have become key challenges for enterprises in every industry around the globe. Cybercrime is taking on ever more and ever new forms – from data theft or forgery to computer sabotage or cyber espionage to improper handling of company information by staff, suppliers, or other business partners. And malicious cybercrime is only part of the problem. Defensive approaches to combat the threat must keep pace. Firms can no longer rely on existing corporate risk management approaches or their IT department's capabilities; they must implement more far-reaching measures. Effective information security is an issue that involves the whole company, and it needs to be established as a permanent item on the board's agenda. The challenges are multidimensional and call for a broad approach to risk assessment. Oliver Wyman has identified the key criteria that determine the success of sustainable information security management.

The success of every enterprise, in all sectors all over the world, is now intimately dependent on the integrity of information and connectivity. According to *Global Risks 2014* published by the World Economic Forum[1], the breakdown of the basic information infrastructure ranks fifth among the risks having the potentially greatest impact on the world economy. And, in the same report, cyber attacks are ranked fifth among the most probable risks in the world.

Especially high-tech economies such as those of Germany, Singapore, or the US are preferred targets of cyber attacks, which are becoming more aggressive and more sophisticated. The Center for Strategic and International Studies has found that, in 2013, cybercrime caused damage of the order of $575 BN globally. Since 2010, the number of registered cyber attacks has risen by more than 20% per year, but by no means all attacks are spotted or reported by businesses.

A MULTIFACETED THREAT

Enterprises are increasingly aware that cybercrime is a serious risk that may even threaten their very existence. Despite this, approaches to dealing with the issue are still too fragmented. Risk assessments primarily focus on traditional external attacks so that adapting the firewall by IT is very often the only protective measure taken. However, information security is far more multidimensional.

Companies who want to protect their corporate data and other assets against unauthorized access or damage must already consider a broad set of both internal and external threat scenarios. These scenarios will only increase as companies undergo digital transformation, which in turn increases the opportunities for cybercrime to impact on shareholder value.

[1] The Global Risks report is compiled once a year by the World Economic Forum in conjunction with Marsh & McLennan Companies and other partners. The study results of the *Global Risks 2014* are derived from a survey among more than 700 experts and examine 31 risks of worldwide importance in the next decade.

EXAMPLES OF CYBER THREATS

SABOTAGE AND TERRORISM

- Aim: to cause maximum damage
- The attacker doesn't necessarily try to disguise their identity
- Desire to attract strong public attention

ESPIONAGE AND CRIME

- Aim: personal gain or advantages
- The perpetrator concentrates on not being identified at all or on being identified as late as possible
- Availability of potentially significant financial and technical resources

OPERATIONAL RISKS

- Indirect risk as a result of the loss of data or associated damage (for example financial losses, competitive disadvantages, image loss)
- Often caused by own employees or external partners
- More of an opportunistic risk – weaknesses are not deliberately exploited

EXTENSIVE DAMAGE

Just as the cybercrime threat is broad, so the potential impacts are multidimensional. Enterprises are already experiencing reputational damage from data leaks, financial losses as a result of production stoppages, theft of business secrets, and operational constraints due to the manipulation of technical equipment. And the impact is not only at the enterprise level. Individual board members and executives can be held responsible and accountable in case of violations or evidence of security deficiencies. It is no surprise that, in a current study conducted by our sister company Marsh, risk managers of large companies mentioned that they are above all concerned about the misuse of customer information, the loss of intellectual property, reputational damage, and, more and more often, regulatory consequences[2].

Against this background, many boards are rightly putting information security firmly on the agenda. They seek to move from case-by-case reactive measures to a balanced portfolio of initiatives that involve the entire organization and align risk management with commercial imperatives. On the technical side, it is important to ensure that unauthorized access to the company's systems is restricted. Moreover, businesses must include sensitizing their workforce to information security in their training programmes. In addition, they must make their organization secure by introducing sustainable leadership structures and leadership mechanisms. Last but not least, processes must be designed in such a way that third parties cannot gain access to company data.

[2] Marsh is one of the world's largest insurance brokers and belongs to Marsh & McLennan Companies. The company is a leader when it comes to protection against cyber risks. Furthermore, Marsh regularly carries out the Cyber Risk Survey.

INSIGHTS FROM HEAVY INDUSTRY

Oliver Wyman developed an information security strategy for a supplier in a security-related heavy industrial sector. The project, which covered the company's entire process landscape, was the responsibility of the IT department. Oliver Wyman, in conjunction with the client, identified the most important security requirements and the necessary measures. The results clearly showed that the key levers for improving security could only be implemented in cooperation with the companies of the supplier's partners and customers. These stakeholders played a critical integrating role for the company's products in more complex (and vulnerable) end systems requiring more sophisticated information security measures. For the measures to be successful, responsibility for the programmes had to be shifted from IT to executive board level.

Lessons learned:

- The degree of vertical integration in the value chain is a key factor for determining a company's level of information security. In many cases, coordination with suppliers and/or customers is necessary.
- In many cases, assigning responsibility for executing an information security project to the IT organization falls short of the mark because key risks and security requirements are often found outside of IT. Consider assigning responsibility for company-wide programmes to the executive board or board.

INSIGHTS FROM THE ENERGY INDUSTRY

An energy company requested that Oliver Wyman evaluate its current information security level, and identify risks and any necessary mitigation measures. In this case, many industry-specific regulations had to be taken into account. Oliver Wyman contributed not only its technical expertise, but also its regulatory know-how to the project. As a result, measures were defined and documented that would both withstand scrutiny by third parties and add protection.

Lessons learned:

- When defining information strategies in regulated industries, it is important to have a profound knowledge of the regulatory environment, which in many cases is evolving rapidly as digitization changes the game.
- Standards such as ISO 2700x and NIST (National Institute of Standards and Technology) provide important reference points and suggestions, but they need to be adapted to the specific situation, industry, and special regulatory provisions – vanilla implementation is not sufficient.

INSIGHTS FROM THE FINANCIAL SERVICES INDUSTRY

Oliver Wyman evaluated and reviewed the cybersecurity roadmap of a leading financial institution, which also led to the identification of weaknesses in the areas of prevention and detection.

Lessons learned:

- Successful protection requires companies to know which of their assets are worth protecting, and what the firm's main security needs are.
- To quickly identify weaknesses, it is necessary to gather and evaluate any relevant risk data and implement far-reaching early detection indicators.
- Cyber intelligence analysis teams should not only collect the data streams of external service providers (for example monitoring of Dark Web/Deep Web pages), but also actively monitor internal systems and processes for weaknesses.
- The same teams should be responsible for coordinating the activities of security authorities, including regularly prioritizing threats and reviewing and updating security measures.

MANY ENTERPRISES ARE PLAYING CATCH-UP

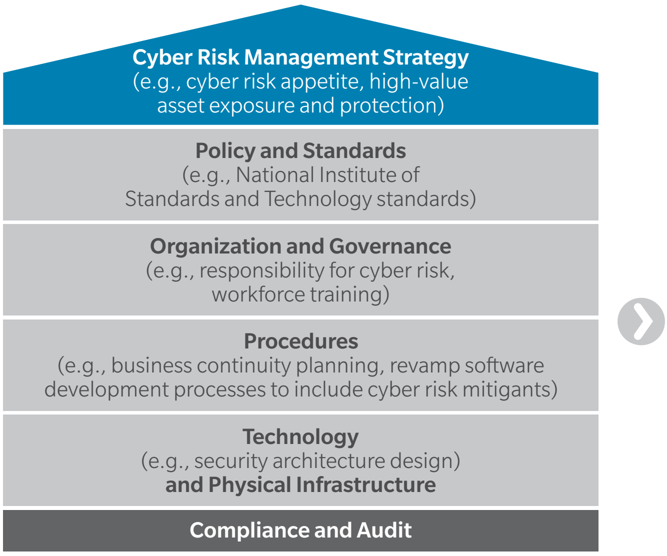
Many businesses have not yet realized the demands for far-reaching, multidimensional information security. Their own risk assessments do not yet call for a holistic approach. In Oliver Wyman's view, this is mainly because there is too little transparency within companies regarding which information and systems really need to be protected. This is no easy task with the need differing from company to company and from industry to industry. While a machinery manufacturer may need to protect construction plans or access data for production equipment, industry service providers or marketing agencies, on the other hand, may need to ensure that their customer data or confidential project information are secure.

To catch up and provide comprehensive security, enterprises will need many functions to collaborate. It is not enough to rely entirely on the IT department's technical capabilities or effective corporate risk management. Because the potential threats and the issues that arise from them are complex and diverse, corporate risk management can only serve as a basis for an effective information security approach. Winners will adapt not only processes and structures, but also basic technical parameters, the corporate culture, and the treatment of employees.

SUCCESS FACTORS

According to Oliver Wyman, there are a number of criteria that make or break the success of sustainable information security. At the top of the list is holistic risk assessment – across all functions and levels – which takes not only potential goals but also threats and measures into account. It is also important to gain clarity on the business's most important information assets and data, namely information, products, areas, processes, or systems that are strategically relevant to the company and must therefore be protected at all costs. At the same time, it is essential to have an eye on how their importance will change as a result of digital transformation or the review of the business design.

Exhibit 1: A company-wide framework for information security management


Cyber Risk Management Strategy
(e.g., cyber risk appetite, high-value asset exposure and protection)
Policy and Standards
(e.g., National Institute of Standards and Technology standards)
Organization and Governance
(e.g., responsibility for cyber risk, workforce training)
Procedures
(e.g., business continuity planning, revamp software development processes to include cyber risk mitigants)
Technology
(e.g., security architecture design)
and Physical Infrastructure
Compliance and Audit

- An overarching **cyber risk strategy** is created based on risk appetite, environment, and capabilities.
- **Governance** structures are installed to control cyber risk and security throughout the organization.
- **Security policies** are derived to guarantee compliance with industry standards (such as PCI, ISO, FISMA).
- Selection of **suitable personnel** and their training.
- Risk culture is established.
- **Security processes** are aligned to the cybersecurity strategy and security policies.
- **Technology infrastructure** is deployed to support the security processes.
- **Physical infrastructure** is designed and installed with access controls, surveillance, and crisis management.
- **Regular audits and war gaming** are conducted to ensure performance and compliance with defined processes.

Source: Oliver Wyman

In addition, it is important for firms to be aware of possible damage scenarios and to determine their risk appetite. Furthermore, they must integrate key information security measures ranging from the definition of a clear strategy for protecting all relevant company information, through the implementation of appropriate governance structures, and to regular audits and process control points that make it possible to assess the extent of a threat at all times.

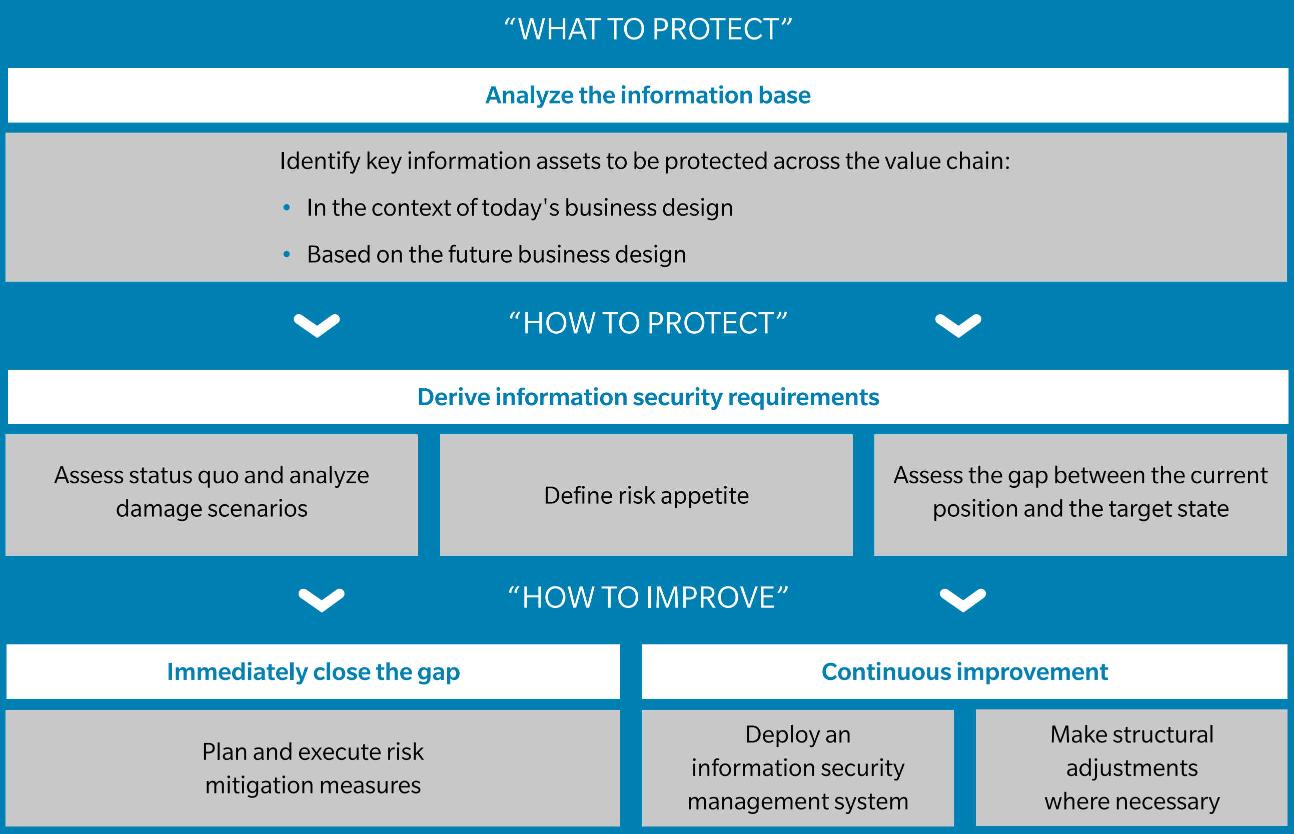
A CONTINUOUS PROCESS

Information security does not mean that an enterprise will achieve optimum security overnight. Although technical improvements can often be implemented quickly, organizational and process changes can take up to one year. In general, sensitizing colleagues through cultural change takes the most time.

Once the foundation has been established, sophisticated information security becomes an ongoing process that fits the activities and size of the company. A corporate security officer is needed for managing cyber risk effectively – in the person of a Chief Information Security Officer, a Data Security Officer with an extended remit, or a board member whose responsibilities are expanded accordingly.

Every company needs to take action immediately. Cybercrime will continue to grow and develop new facets. Companies who do not address this development with holistic information security management are at greatest risk.

Exhibit 2: Information security procedure



"WHAT TO PROTECT"

Analyze the information base

Identify key information assets to be protected across the value chain:

- In the context of today's business design
- Based on the future business design

"HOW TO PROTECT"

Derive information security requirements

Assess status quo and analyze damage scenarios

Define risk appetite

Assess the gap between the current position and the target state

"HOW TO IMPROVE"

Immediately close the gap

Plan and execute risk mitigation measures

Continuous improvement

Deploy an information security management system

Make structural adjustments where necessary

Source: Oliver Wyman

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across 26 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm's 3,700 professionals help clients optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC].

For more information, visit www.oliverwyman.com.

CONTACT

DR. CLAUS HERBOLZHEIMER

Partner, Strategic IT & Operations
claus.herbolzheimer@oliverwyman.com
+49 30 399 945 63

DR. KAI BENDER

Partner, Strategic IT & Operations
kai.bender@oliverwyman.com
+49 30 399 945 61

SILVIO SPERZANI

Partner, Strategic IT & Operations
silvio.sperzani@oliverwyman.com
+39 23 057 7449

OLIVER WYMAN